Amendments to the Claims:

Please amend the claims as indicated.

1. (Currently amended) An apparatus for secure computer readable medium backup, the apparatus comprising:

a computer readable medium having at least a first accessible portion and a second encrypted portion; and

a trusted platform interface module operatively coupled with the computer readable medium and configured to communicate with a cryptographic module, wherein the trusted platform interface module comprises a password module, the trusted platform interface module initializing the password module in response to verifying the cryptographic module by comparing a known value stored on the password module to a cryptographic module platform configuration register value storing a hash of POST BIOS code, wherein only the cryptographic module may initialize the password module, the password module configured to store and transmit an encrypted password to the cryptographic module, and receive an unencrypted password from the cryptographic module.

2. (Original) The apparatus of claim 1, wherein the cryptographic module comprises a trusted platform module (TPM).

3. (Original) The apparatus of claim 1, wherein the computer readable medium comprises a computer readable peripheral selected from the group consisting of a hard disk drive, a universal serial bus storage device, a floppy disk, an optical storage disk, a flash memory storage device, and a network attached storage drive.

4. (Canceled)

5. (Currently amended) The apparatus of claim [[4]]5, wherein the encrypted password comprises a unique password configured to be decrypted by the cryptographic module that first created the encrypted password.

6. (Original) The apparatus of claim 1, wherein the computer readable medium module further comprises a backup utility module configured to selectively copy data from a storage device source, detect newer versions of data stored on the storage device source, and replace older versions of the data on the computer readable medium with newer versions of the data.

7. (Currently amended) A device for secure computer readable medium backup, the device comprising:

a motherboard; ~~and~~

a cryptographic module coupled to the motherboard and configured to communicate with a computer readable medium[[.]]; and

the computer readable medium comprising a trusted platform interface module configured to communicate with the cryptographic module, wherein the trusted platform interface module comprises a password module, the trusted platform interface module initializing the password module in response to verifying the cryptographic module by comparing a known value stored on the password module to a cryptographic module platform configuration register value storing a hash of POST BIOS code, wherein only the cryptographic module may initialize the password module, the password module configured to store and transmit an encrypted

password to the cryptographic module, and receive an unencrypted password from the cryptographic module.

8. (Canceled)

9. (Currently amended) The device of claim [[8]]7, wherein the cryptographic module is configured to receive the encrypted password from trusted platform interface module, decrypt the password, and transmit the decrypted password to the trusted platform interface module.

10. (Currently amended) The device of claim 7, wherein the cryptographic module comprises a ~~trusted platform module (~~TPM[[)]].

11. (Currently amended) The device of claim 7, wherein the motherboard further comprises a memory[[,]] and a processor coupled to the memory.

12. (Original) The apparatus of claim 7, wherein the computer readable medium comprises a computer readable peripheral selected from the group consisting of a hard disk drive, a universal serial bus storage device, a floppy disk, an optical storage disk, a flash memory storage device, and a network attached storage drive.

13. (Currently amended) A system for secure computer readable medium backup, the system comprising:

a motherboard;

a cryptographic module coupled to the motherboard configured to decrypt encrypted passwords;

a computer readable medium module having at least a first accessible portion and a second encrypted portion; and

a trusted platform interface module operatively coupled with the computer readable media module and configured to communicate with [[a]]the cryptographic module, wherein the trusted platform interface module comprises a password module, the trusted platform interface module initializing the password module in response to verifying the cryptographic module by comparing a known value stored on the password module to a cryptographic module platform configuration register value storing a hash of POST BIOS code, wherein only the cryptographic module may initialize the password module, the password module configured to store and transmit an encrypted password to the cryptographic module, and receive an unencrypted password from the cryptographic module.

14. (Canceled)

15. (Original) The system of claim 13, wherein the encrypted password is configured to be decrypted by the cryptographic module that first created the encrypted password.

16. (Original) The apparatus of claim 13, wherein the computer readable medium further comprises a backup utility configured to selectively copy data from a storage device source, detect newer versions of data stored on the storage device source, and replace older versions of the data on the computer readable medium module with newer versions of the data.

17. (Currently amended) A computer readable storage medium comprising computer readable code configured to carry out a method for secure computer readable medium backup, the method comprising:

providing a computer readable medium having at least a first accessible portion and a second encrypted portion;

initializing a password module in response to verifying ~~according to unique data stored within~~ a cryptographic module by comparing a known value stored on the password module to a cryptographic module platform configuration register value storing a hash of POST BIOS code, wherein only the cryptographic module may initialize the password module;

transmitting an encrypted password to the cryptographic module;

authenticating the encrypted password;

decrypting the encrypted password;

transmitting the decrypted password to the computer readable medium module; and

decrypting the second encrypted portion using the decrypted password.

18. (Original) The computer readable storage medium of claim 17, wherein the method further comprises copying data from a source storage device, and storing the data in the second encrypted portion of the computer readable medium.

19. (Original) The computer readable storage medium of claim 17, wherein the method further comprises restoring data to the source storage device from the computer readable medium.

20. (Canceled)

21. (Original) The computer readable storage medium of claim 17, wherein the method further comprises storing and transporting data in the accessible portion of the computer readable medium.

22. (Currently amended) A method for secure computer readable medium backup, the method comprising:

providing a computer readable medium having at least a first accessible portion and a second encrypted portion;

initializing a password module in response to verifying ~~according to unique data stored within~~ a cryptographic module by comparing a known value stored on the password module to a cryptographic module platform configuration register value storing a hash of POST BIOS code, wherein only the cryptographic module may initialize the password module;

transmitting an encrypted password to the cryptographic module;

authenticating the encrypted password;

decrypting the encrypted password;

transmitting the decrypted password to the computer readable medium; and

decrypting the second encrypted portion using the decrypted password.

23. (Original) The method of claim 22, further comprising copying data from a source storage device, and storing the data in the second encrypted portion of the computer readable medium.

24. (Original) The method of claim 22, further comprising restoring data to the source storage device from the computer readable medium.

25. (Canceled)

26. (Original) The method of claim 22, further comprising storing and transporting data in the accessible portion of the computer readable medium.

27. (Currently amended) An apparatus for secure computer readable medium backup, the apparatus comprising:

means for providing a computer readable medium having at least a first accessible portion and a second encrypted portion;

means for initializing a password module in response to verifying~~according to unique data stored within~~ a cryptographic module by comparing a known value stored on the password module to a cryptographic module platform configuration register value storing a hash of POST BIOS code, wherein only the cryptographic module may initialize the password module;

means for transmitting an encrypted password to the cryptographic module;

means for authenticating the encrypted password;

means for decrypting the encrypted password;

means for transmitting the decrypted password to the computer readable medium module; and

means for decrypting the second encrypted portion using the decrypted password.

28. (Original) The apparatus of claim 27, further comprising means for copying data from a source storage device, and storing the data in the second encrypted portion of the computer readable medium.

29. (Original) The apparatus of claim 27, further comprising restoring data to the source storage device from the computer readable medium.

30. (Canceled)